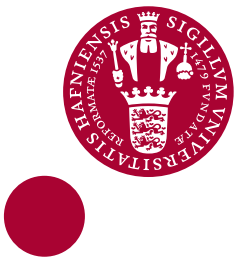

Vision, faces, identities

Technologies of recognition

Møhl, Perle

Published in:
The Biometric Border World: Technology, Bodies and Identities on the Move

DOI:
10.4324/9780367808464

Publication date:
2019

Document version
Other version

Vision, faces, identities: technologies of recognition

by Perle Møhl

In: *The Biometric Border World: Technology, Bodies and Identities on the Move.* Olwig, K. F., Grünenberg, K., Møhl, P. & Simonsen, A. (eds.). London & New York: Routledge, p. 83–99.

This chapter analyses technologies of border control that operate through *recognition*. The technologies are used in various border settings, but are united by a shared techno-temporal quality, namely that they identify persons and objects by comparing them to *already registered* IDs and *already known* threats. The chapter will first describe the principles and visual skills involved in running the Automated Border Control system in Copenhagen Airport, comparing them with face-to-face ('manual') border control and random checks on intra-Schengen flights. Secondly, the use of an X-ray scanner to determine the contents and possible threats of passenger luggage in Gibraltar Airport will be analysed. In all these cases, humans and machines deploy refined and often interlaced visual and sensory skills or methods to determine whether a person or an object may pass or requires further scrutiny. This work engages with a complex combination of data, recognition and memory, and sensing and sensory skills that come to be mutually formative. The machinic operations are largely based on and formed according to human capacities and at the same time format how and what the humans operating the technologies come to sense and see, as well as 'unsee', in an interplay of continued enskillment *and* deskillment. We could tentatively characterize this integrated human-technological border assemblage as cyborgian (Haraway, Wolfe, and Haraway 2017; Wells 2014) in that human and technological processes and sensory connections supplement and reinforce one another. But, as we shall see, they sometimes also destabilize one another's operations and skills and work in more contested and disconnected ways, thus undermining the analytical pertinence of the connected symbiotic cyborg.

The chapter further analyses the kinds of *suspicious relations* – notably between faces and identities – that arise and undergo scrutiny in border control and the *thresholds of resemblance* that are required to pass border control: that is, how much one needs to resemble one's ID photo. Finally, the chapter presents a particular element of airport

security control where known threats appear artificially on the security agents' screens to check not the luggage itself but the skills and alertness of the agent. In all these examples, sign relations are established between objects and meanings. On the surface these relations appear simple and direct, but they are in fact enmeshed in and enskilled through a complex political, economic and social community of practice. The chapter attempts to single out a few of these semiotic operations, the forces they are regulated and influenced by, and the effects they have on the production of identities, threats and borders.

Settings and technologies

As mentioned in the introduction to Part II, I carried out fieldwork with border police in three main settings: Copenhagen Airport, Gibraltar Airport and the territory's land border with Spain, and in Ceuta on the border between Spain and Morocco. The goal was to analyse the different types of technologies that were used to detect and deter threats and to compare their workings. The border control processes I present in Chapter 4 concern different forms of *presence detection* used mainly in Ceuta. In the two airport settings, however, control was to a large extent technologized and automatized, and control of identities and objects took place through processes of identification and recognition, as we shall see.

This chapter therefore takes us to the two airport settings, starting with the Schengen passport control in Copenhagen Airport. Here police and civil border guards supervise the running of an automated facial recognition system devised and installed by the Portuguese company Vision-Box and maintained by a Danish service company, Biometric Solutions. The system is called the ABC – Automated Border Control – and consists of nine 'eGates', three of which can be adjusted for use from both sides to accommodate different passenger flows. Besides the automated eGates, the border zone also consists of a row of 'manual' passport control booths where border guards physically check passports and visas. Specifically for migration control objectives, police officers also carry out random checks on intra-Schengen flights arriving from so-called 'high-risk' cities in southern Europe. After describing and analysing the sensory and interpretive work involved in these operations, the analysis then moves to Gibraltar Airport, where police officers survey the screens of X-ray scanners, inspect passenger luggage, detect

possible threats, make assumptions about the identities of the travellers from the objects they can identify, and assess whether it 'all makes sense'.

In all these cases, the border guards are presented with imagery, scans, objects and faces that they need to single out, identify and assess in a series of complex human–machine interactions and intricate processes of reading and interpreting signs. These readings are based on already identified threats, as well as on assumptions about the translucence and authority of the images and their direct relation to specific persons, objects and lives.

The analysis in this chapter is based on fieldwork conducted in Copenhagen Airport and Gibraltar Airport over a period of five months during 2016-2017.

Facial recognition and looking like a picture

At Copenhagen Airport, Hanne, a border guard, is surveying her two screens. She has turned on the computer and the ABC system that monitors the eGates, has logged into the system and has opened the access to the different national and international police databases (national ID, watch lists, wanted persons, etc.). She activates the six eGates she is in charge of, and the green lamps turn on, inviting the first travellers into the ABC. From her little glass booth, Hanne has an overview of all the gates and the travellers passing through them. She picks up her mouse and starts working, shifting her attention between the ABC screen, the faces and bodies of the travellers, and the database screen when something appears on it. With a click, or using the touchscreen, she can 'help' the ABC, checking the irregularities it identifies, overriding it when it makes mistakes and turning it off when it 'starts glitching'. Otherwise she simply checks that it 'does its job'. She is in radio contact with her colleagues on the floor and in the other control booths and can tell them when she sees something suspicious – people changing queues or looking nervous, or switching from the ABC to the manual control booths.

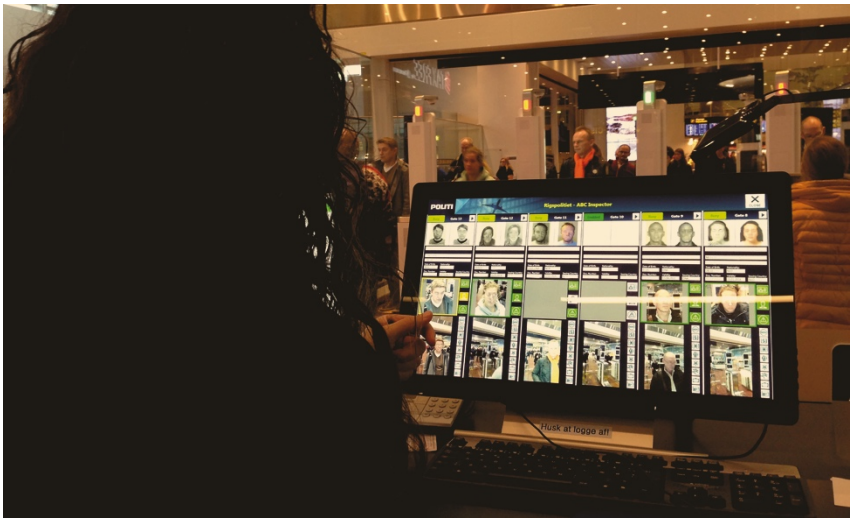

Figure 1. Comparing 2D photos to 3D faces in the ABC control booth (© photo by the author)

The ABC uses a facial recognition system where the ID photo in the biometric passport is compared to the face of the person passing through the control. The passport contains a so-called 'template' of the facial features of the ID photo, that is, a series of measurements of distances of key points in the photographed face. In passing through the eGate the same features are measured on the traveller, and a new template is produced and compared to that from the ID photo. Thus, contrary to human recognition, algorithmic recognition does not compare actual faces to photographed faces but templates extracted from both. Comparing the template from the photo and the one from the live face, the ABC algorithm produces a comparison score that has to meet a certain threshold for the exit door to open. The score can range from 100 – total resemblance – to 0 – no resemblance whatsoever. And it actually does vary quite a lot while Hanne is looking at her screen.

Hanne is a senior police officer who has been working in the ABC since it arrived five or six months previously. She is a 'super-user', training newcomers, and she likes working with the ABC, defending 'it' vehemently when a colleague launches into criticism of it during a break or when I ask her. She finds it amusing, even touching, when it mistakes a suitcase for a second person, when it can't see because of the sunlight, or when 'it gets confused' and starts glitching. She talks to it and often laughs, describing it as having a consciousness, moods and sensory frailties that resemble her own, as when humans ascribe consciousness and will to their computer to explain its intricacies and

malfunctions (Jackson 2002). To her colleagues' objections that in the end it will make them all useless, she says 'Well, it can be turned off. We can't.' She is confident that human skills will always be indispensable in border control. She will be retiring from the service in a couple of months, a year at the most – which might explain why she does not feel menaced by the machine as some of her younger colleagues do.

A traveller arrives at the entrance to the eGate, places his biometric passport on the scanner, and the passport is read by the ABC system. After some moments the passport photo and the chip photo, as well as the contained ID information, appear on Hanne's screen. If the two photos are identical – that is, if the picture in the passport hasn't been replaced with another one – and if the passport is biometric, undamaged and in compliance with the ABC system, the first glass door automatically opens, and the traveller is invited into the eGate. Up until now, only the passport has undergone scrutiny. Now it's time to check that the person in the document and the person in the eGate are the same – or, rather, that the face in the document and in the eGate look sufficiently alike.

The traveller is asked to stand on a pair of yellow footsteps on the floor, the entrance door closes, and the traveller is trapped inside the eGate with no possible escape route. The camera moves up and down, small lamps blinking, and finally settles in front of the traveller's face. What goes on in the entrails of the ABC – what it sees, what it is doing, thinking or processing, which databases it is linked to and checking right now, what it remembers – all that is invisible and unknown to the traveller, who just waits in front of the camera and the closed door. From her position in the ABC booth, Hanne can check the ABC's algorithmic operations on her screen by making a line of algorithmic operations appear in a little window next to the facial images of the traveller. Prompted by my question, she opens the operations list and admits she has never really looked at it before and doesn't know how to read it. She has up to six gates to survey and no time to check what the ABC is doing, as long as it is running smoothly and showing no alerts of detected irregularities or 'signs of fatigue', as she says.

The live face of a traveller in the eGate shows up on Hanne's screen, and the ABC starts comparing the facial templates from the passport with the direct cameras. If the comparison score is high enough, meeting the 'recognition threshold' – usually

somewhere between 40 and 50, depending on the settings – the gate will open, and the person has successfully passed the border. But it does not always go that smoothly. The ABC system is hyper-sensitive, Hanne says, and if one eGate starts having problems, it sometimes spreads from one gate to another 'like a viral infection'. If there's too much light or too little, or if people are moving around or are carrying a lot of bags, it 'can't see properly'. Often a second-line police officer has to step in to indicate the right position and posture if the traveller doesn't comply with the system's specifications. 'Stand still, not too close'. 'Take off your glasses'. 'Take off your hat'. 'Remove your veil'. 'Look at the camera' – modifying their appearance until the door opens.

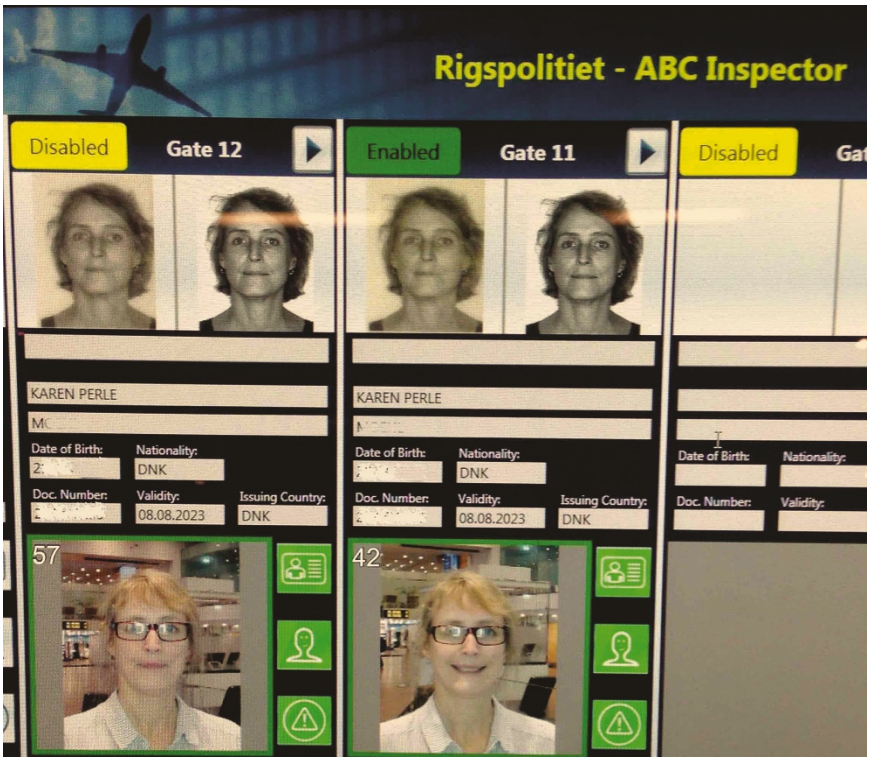

Figure 2. The author in the ABC, trying to look like the ID photo, more or less successfully(© photo by the author).

Thus, in fact, to pass through the ABC requires that one looks sufficiently like the face in the ID photo, whether the passport is one's own or someone else's. The little ABC enclosure becomes a theatre of inquisition where one is under suspicion until the algorithm has finished analysing and comparing faces and templates, and the glass doors open. On this stage, people are told straighten their hair, smile or stop smiling, in order to 'look sufficiently' like the photo to meet the threshold of resemblance. The ABC is

reacting directly to their capacity to look like the face in the photo, displaying the changing comparison score – …13…35…22…44! – as the face in front of the camera changes appearance. The ID photo itself has been formatted for the occasion of making the passport, with strict instructions on how to look and how not to look.[1] More than a site of identification, the ABC becomes a scene of semblance, of mimicry, of creating an iconic likeness with the photo – a photo that is an already formatted version of a face, often captured many years earlier. Thus the recognition system, whether automated or human, is based on the comparison between a supposed original – which here ironically becomes the ID photo – and a suspicious-until-verified replica, the face of the traveller.

Inversely, what the ABC and the border guards are assessing is not the identity of a person in all his/her social and existential intricacies – something that could never be transformed into simple ID information (Feldman 2013; Møhl forthcoming) – but the travellers' skills in iconicity and mimicry of a small 2D photographic version of a face. All authority is vested in this small simulacrum and in its indexical relationship to a particular ID, and control consists in the capacity of the algorithms and the border guards to see and read it, to re-cognize the ID-face in the living face. One could argue that the ID photo has taken over the identity – or at least the ID – of the person who was originally photographed. The photo has become the original to which the traveller must conform, whether it is her/his own or someone else's passport. As Susan Coutin observes, to pass a border, one becomes eligible by producing the adequate documents, for 'documents confer, rather than derive from, statuses' (Coutin 2003: 60). A person can 'claim an identity' simply by waving a document, as a frustrated border official remarked to Gregory Feldman (2013: 142). As such, the simplest way to derive an adequate status and pass the border is, Coutin notes, to purchase fraudulent documents. Or, since the introduction of biometric passports in Europe, to purchase valid biometric documents with ID photos with which one can produce a reasonable level of resemblance, just as long as there is a valid document and, in my analysis, an ID photo with which to conform. As such, it is the capacity for resemblance and mimicry that confers status.

Indeed, documents *can* be tampered with, photos *can* be replaced. But the DocuUnit at the airport police department teaches the border guards to detect forged documents and passports, and they are pretty good at it. They learn to see the irregularities in the

printing, the cuts and tears, the missing watermarks, to feel the stitching, the thickness of the pages and the embossing, and to listen to the sound of the plastic when tapping it with a nail or on the desk. The differences are minute and imperceptible to the untrained, but the border guards' enskilled senses are proficient in these matters. And in the ABC, the algorithm compares the visible ID photo to the chip photo to determine if they are identical. So, forged documents are becoming a rarity, especially since the introduction of biometric passports. Instead, the most common document fraud currently detected in Copenhagen Airport is not persons travelling on forged documents, but rather on another person's *valid* document – 'impersonation' (Frontex 2013). This is confirmed notably by our research among migrants (see Chapters 6-7) who prefer to travel on borrowed or bought legitimate documents when trying to pass border control. All it takes is to look sufficiently like the person in the small ID photo.

On this little stage of mimicry and unmasking, the border guards employ their own personal tactics. Hanne has been working with the ABC since it was installed and is gradually adjusting her senses to the work of the machine. As she says, 'I'm learning to see in 2D', comparing the 2D screen photo to the actual '3D' face in the eGate. She enjoys trying to outsmart the machine, 'seeing more quickly' than the machine, making her identity assessment before the ABC opens its doors and sets the traveller free. And to do that, she says, she has to 'see like the machine'. According to this logic, her vision is being transformed by adapting it to the ABC's vision and scans of small ID photos, switching between the depth of living, changeable, fleshy faces in front of her and the black-and-white imprints of their superficies. She is *learning to see* in *other ways*, her vision is being formatted by how the ABC sees and by the materiality of photographic technologies and how they work and convey knowledge – how they epitomize and essentialize identities by linking those fleshy faces and bodies to the data in the document.

I ask Hanne if she thinks the ABC sees better and is more efficient than humans. She is not sure, she says. 'No one is foolproof, not the machines nor the humans'. She alludes to the predicament that no one can know how many have actually managed to fool passport control. 'How could we know? They went unnoticed!' Then, to make her point, she tells me that some days earlier an airline agent prevented a traveller from boarding

a flight because he was trying to travel on another person's passport. Yet he had made it through the manual passport control. The officers of the DocuUnit apprehended him and, while they were at it, ran him and the passport through the ABC three times to see how it reacted, and he actually almost passed once. The case speaks directly to the overarching predicament of nescience in policing and security: never knowing who wasn't stopped, how many went unnoticed. But Hanne keeps the discussion at a more practical level: 'People who want to cheat probably don't choose the ABC. I'm not sure it works better, but apparently people think it does, so they chose the human border guard…' She concludes, 'It depends on a lot of things. Sometimes the machine sees better, sometimes the human eye does'.

Figure 3. When the ABC starts glitching, there are several solutions; one of them is to turn it off (© photo by the author).

Indeed, when I have seen cases of obviously different faces in the ABC and in the scanned passport, it has always been someone who accidently took the wrong passport, for example, couples inadvertently switching passports just before going into the ABC or, as happened once, someone who took his mother's passport with him. Or a border guard checking that the ABC is up and working, as one of them does every morning when he starts his guard by trying to pass through the ABC using a prop passport and grimacing to mimic the ID photo of a rather chubby man. Through this routine check, he also seems to be assuring himself that the ABC – and with it, the whole service –

can't be fooled, that it is still sufficiently on guard and, importantly, that the recognition threshold has not been lowered overnight. In sum, he checks that the border is still there and working.

In the ABC, ID photos play a major part in the work of border control. The ABC itself 'looks at' and compares faces with ID photos, the border guards in their booth do much the same, keeping pace with the machine, and everything is to a large extent based on the indexical authority of the photographic image to contain and convey the truthful link between face and identity.

Hanne's enskilled vision plays a huge role. But she also uses her other senses, listening to the sounds in the room and on the radio, surveying the bustle and the reactions of people in the queues. This multi-sensoriality becomes even more acute when she moves over to the manual passport control.

'Manual control', making sense and questions of plausibility

In both the ABC and the manual control booth, the border guards use their eyes to look at passports, photos, faces, behaviour: who is looking nervous, changing queues, etc. But in the 'manual' control, the border guards sit close to the travellers and deploy '*all* their senses, including the sixth', as Ole, one of Hanne's colleagues says. And in the manual control, Ole adds, they are not restricted, as in the ABC, to controlling travellers on the basis of already registered images and data. In the manual control they can pry into the future, they can use their 'creativity and intuition'. 'You can have people whose papers are perfectly in order, but who behave strangely'.

I sit in with Ole and Hanne in their joint manual control booth in a border zone where flights arrive from extra-Schengen airports defined as 'high-risk'. Arriving passengers are separated from other passengers by an intricate network of corridors that sends them to an extra security check and a secluded baggage reclaim because they are arriving from airports where security control is considered insufficient by Schengen standards.

Ole and Hanne comment on their work as the travellers arrive, giving a sense of the variety of their sensory work. They check heights using an old-fashioned height-meter. They look – down at the document, up at the face, out at the queues, down, up, out. They listen to voices, explanations, intonations, accents. They touch the passports, feel

the stamps, the stitching and embossing, the newnesses and the wear-and-tear. They smell smells. They ask questions: 'Where are you going?', 'What is your purpose there?', 'Who are you visiting?' They chat about destinations and origins, about the travellers' children, about the weather. They scan passports, fingerprints and make photocopies. And while they are doing all that, in the twenty seconds or less that they have at their disposal for each traveller, they stitch together all the minute details they pick up, weaving the fragments into stories about the travellers' intentions and agendas, and assessing the plausibility of those stories and whether they make sense or not, or, as Ole and Hanne put it, 'whether two and two make four – or five'. They are pre-empting, thinking ahead, imagining and assessing potential threats – that is, events in the future – based on the thickness of the here-and-now, and not only on sparse ID data from the past and a small ID photo. Unlike in the ABC booth, they work with their versatility, their capacity to cognize, to improvize, to combine disparate details and imagine scenarios about unknown futures. Ole definitely prefers the manual control and the human contact it requires: 'The machine can't think. It's stupid and can only obey orders given by humans. It can't think ahead. I have intuition, I'm creative.'

The way they look at people here is different, 'more full-scale', as some of them say. This is because they deploy *all* their senses in a synaesthetic manner where the senses collaborate to thicken the appreciation and perception, and because in the direct interaction they can 'read' people in more dimensions: temporally, with regard to their past movements and their intentions, and socially, in their interactions with others and in the ways they perform and present themselves. The enskillment of the border guards' senses is not, as in the ABC, formatted by a particular technology that they learn to see through and that they also have to watch over, surveying its modes of vision, its visual impairments and its viral infections.

Analysing vision and sensorial-aesthetic relations with the farming landscape in Normandy, Judith Okely distinguishes between a distant, unengaged gaze and a seeing that involves the entire body and all the senses, and that is based on years of practice and physical bodily engagement with the landscape (Okely 2001). When Okely looks at the agricultural landscape, she searches for 'significance in everything encountered' (ibid.: 111), as I do when I look at luggage scans and travellers, and search for meaning

in every sign. She and I have not yet been trained to focus selectively on particular elements. In border control, as in farming – as in every 'community of practice' (Grasseni 2007a: 203) – there are particular ways of seeing and identifying significance. In border control, training programs are set up to teach the border guards and security officers *what to see* and *what not to see*, notably when looking for details in a passport and scrutinizing a face. Cristina Grasseni, working with cattle breeders who really know how to look at a cow, operates with the same fundamental distinction between distant and immersed forms of vision. She describes 'good looking' as a trained perception, a cognitive form of apprenticeship that is culturally inculcated and socially performed (Grasseni 2007b), a schooling of the eye that 'is at once aesthetic, moral, functional, and normative' (Grasseni 2018).

The political and ideological background of border control and the way the particular border is defined and determines threats and intruders form a basic setting for all the border guards' work, whether in the ABC or in manual border control. But the technological, material and sensory aspects of the different work stations and tasks seem to play just as important a role in the way the guards perform their tasks and how they define and detect threats.

In the following, we accompany a couple of border guards on another type of 'manual' mission in order to examine how it is mainly the *organizational* framework of that mission that makes the border guards *see* in yet other ways and focus on other objects, aspects and appearances than they do in the ABC and the manual control booth.

'Random checks' on 'high-risk flights': looking like a suspect

Border police officers in Copenhagen Airport carry out a certain number of random ID checks every day on flights arriving to Copenhagen from other Schengen countries, which are normally exempt from border control. These checks are audited by police management, both to monitor that the checks are being done and to document the number of weekly checks in case Frontex,[2] the European border control agency, controls their activities.

Walking to the airport terminal used by budget airlines, where we will await the arrival of a plane from an Italian city, I accompany Hans, a short and sturdily built police agent, and his new female colleague, who is carrying out this type of arrival check for

the first time. Hans explains the principles to her as we walk: 'We're looking for illegal immigrants. So we don't stop 'Mr and Mrs Hansen'.' She nods and seems to know what she is required to look for. While we wait for the plane to dock, I ask Hans how he can see whom to pick out if he can't stop everyone. He has some techniques, he says. He can, for example, detect undocumented Afghan men without checking their passports: 'They try to blend in but always look sort of inept-smart. You know, jeans with holes in them. Sunglasses. And there's always something with the shoes – they never fit the rest. Too fancy.'

The flight arrives, and they take up position in front of the arrival gate. Most passengers seem to be Danish tourists coming home. But four men, arriving one by one, could be of African origin. The first is pulled aside by Hans and, having observed him, his colleague pulls aside the next one and asks him to produce his documents. None of them put up any resistance. A third man is stopped by Hans, and a fourth passes by while the officers are preoccupied with the others. All the ones they check have valid documents. Hans smiles jovially and wishes them a welcome home or a continued good trip. He notes down the flight and number of the checked persons on a piece of old wrapping paper – 'So the officer on duty can enter it into the system' – and the two walk off to the other end of the airport to 'randomly' check another flight.

Thus, what sorts of factors play a role in and frame what Hans and his colleague see and how they make distinctions in the task they are being asked to perform? Rather than personal choices and prejudices, it seems to be the notion of 'high-risk flights' that configures which persons Hans decides need to be checked and which persons to let pass. 'High risk' is used in a double sense by Frontex: 1) as a way to optimize resources by concentrating them on flights arriving from European regions of high migration influx (European Commission 2017a), instead of indiscriminately checking every flight – that is, in an organizational sense; and 2) when referring to passengers' specific places of origin, that is, in a geographical sense. At Copenhagen Airport certain flights are therefore defined as high-risk because they arrive from cities within Schengen that Frontex and the national authorities consider possible avenues of 'illegal migrants' and refugees from the Middle East, Asia and Africa. When Hans and his colleagues randomly control such flights, the notion of 'high risk' therefore comes to relate to the countries of

origin of the possible migrants and asylum-seekers, meaning that they are in fact profiling nationalities and not just checking 'randomly'. The notion of 'high risk' therefore logically, including for the border police officers themselves, implies that they are required to check 'people who *look* high-risk', which in this case means 'from Africa or the Middle East'. And, as several officers have said to me, this is paradoxical because it makes them take decisions based on what effectively amounts to 'ethnic profiling'.[3] And even if they might want to contest the legality and ethics of these random checks that are making them select people based on how they look, the border control unit needs to do a certain number of random checks every week for future Frontex controls. As one border guard said, 'If I wasn't a racist before, this work is turning me into one'. Her personal opinion of certain ethnic groups had not changed, she said, but she was de facto required to be more suspicious of certain categories of passengers than of others based on their external physical appearance. She was being asked to apply a synoptic 'tunnel vision' and to 'see like a state' (Scott 1998: 11) – in this case, a union of states, the EU – and not like a human being.

In this example, the technologies involved are not material in kind but infrastructural, involving a range of EU policies and management orders, as well as the travel routes and modalities of migrants, which all contribute to establishing a particular form of legibility (ibid.) and set the conditions for how the border guards deploy their senses, what they look at and how they make decisions based on their visual perceptions. A pair of shoes that are too fancy or a particular kind of face or skin colour will raise the border guard's perceptions above the suspicion threshold and provide the incentive to control the traveller.

In a final example of recognitive skilfulness from my fieldwork at the Gibraltar Airport, we will see how border police use X-ray scanners to look through the surfaces of travellers' luggage in search of threats. This example demonstrates how they are required to both *see* and *unsee*, and how their vision is being both skilled *and* deskilled by a mesmerizing system that is intended to keep them awake and alert to threats – specific *known* threats, that is.

Luggage scans, TIPs and the deskillment of vision

In a secluded room at the bottom of the Gibraltar Airport terminal building, Veronica, a police officer, is surveying her screen. This is Security Level 2. There are no windows, and the artificial light is faint. She is sitting by a long desk, the only piece of furniture in the room except for a couple of chairs. She offers me one and seems content to have company. Somewhere else in the building, on Security Level 1, an automated X-ray scanner checks all luggage before it is sent down to the loading area. If the scanner identifies a suspicious object or an unidentifiable mass, it loads the piece of luggage onto a special conveyor belt, and an image of the piece of luggage pops up on the screen in the cellar. Here, Veronica has exactly twelve seconds to inspect the image. She can either validate the contents as nonthreatening by hitting the green button on the screen, sending the piece back into the ordinary flow of luggage headed for the airplane, or, if she sees a threat or has doubts, she will hit the red button and send it on to Security Level 3. If she does not make a validation within the twelve seconds, it is taken as an indicator that she is either in doubt or inattentive, and the machine automatically sends the luggage on to the next, higher security level.

In another room, Security Level 3, in the midst of the conveyor belts, Veronica's colleague John receives the pieces of luggage that Veronica, or the automated system, have sent on for further inspection. John receives less luggage and has more time to look and reflect. He can turn the luggage X-ray image around, inspect it from all sides or move through the layers, and he has the time to see and identify particular objects to make his decision. But back in Level 2, Veronica only has her twelve seconds to look at the image and figure out why the automated system on Level 1 has deemed the piece suspect. She can use different filters to discern organic from non-organic and metal from soft materials, all displayed in different colours. But she rarely looks at what is inside the piece of luggage. She only has the time to register the blurry zones, the questionable unknowns, and to check for a couple of known threats – explosives, electric circuits, firearms – before hitting one of the buttons. She doesn't actually *see* what is in the piece of luggage, she says – at least in the sense of remembering or being able to list it, attaching meaning to it. She is incapable of telling me what was in the last suitcase when I ask her.

We both look intently at the screen searching for threats as the pieces of luggage pass by, one after the other. 'I have never seen an actual gun or bomb', Veronica says. But she knows they will show up once in a while and that she has to be on her toes. Indeed, at regular intervals – every ten minutes or so – the machine produces a so-called 'TIP', a 'Threat Image Projection', an X-ray image of a known security threat projected onto a piece of luggage.[4] Veronica has to identify the threat and hit the red button within the twelve seconds. 'This is to keep me alert', she says, adding that it is also designed to check that she is doing her work properly and not sleeping. The results of her clicks on the TIP items are registered and presented to her at the end of the month and can lead to reprimands, she says.[5] After some minutes, a suitcase arrives with an unmistakable gun inside; she hits the red button, and the image disappears. 'You saw it?!', she asks. I did. There was something uncanny about it. But I couldn't say what, as it disappeared so quickly.

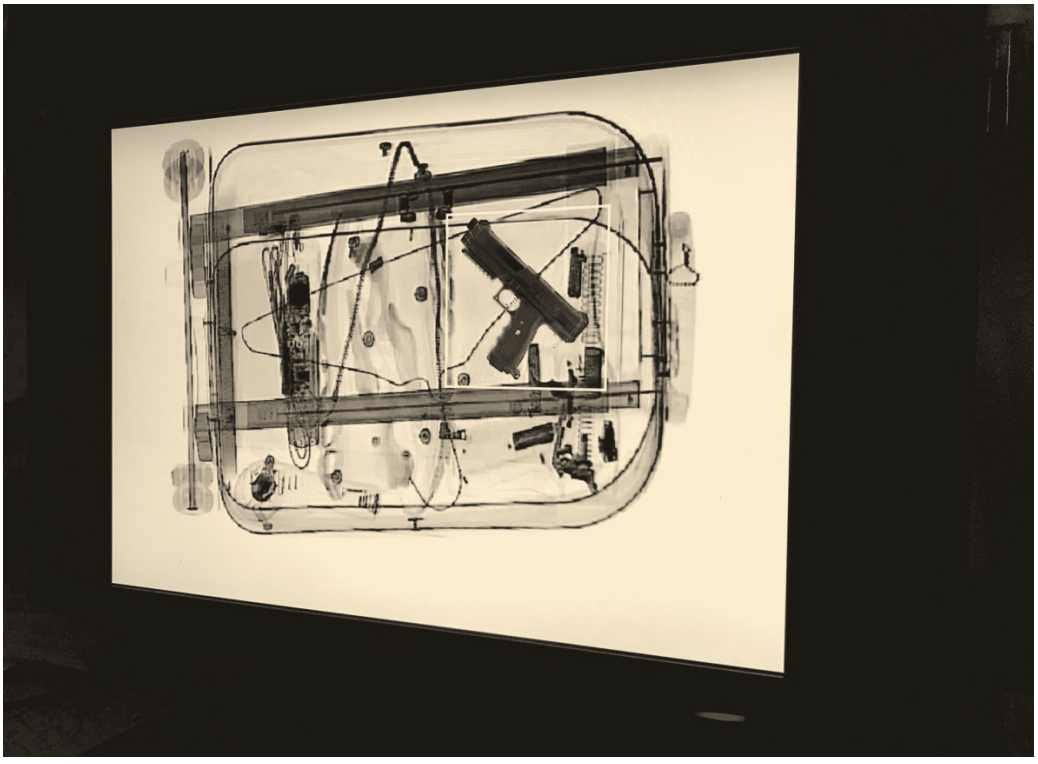

Figure 4. Example of a TIP image (Threat Image Projection) (© photo by the author)

The TIP system is in principle intended to counterbalance the routinization of the selective vision (Cutler and Paddock 2009) and a correlated unseeing because threats so

rarely, if ever, appear in actual traveller bags and thus on the screen. It is therefore intended to ensure that officers are regularly exposed to threats – albeit imaginary threats – so that their vision may be enskilled to seeing those threats, despite the lack of direct perceptions of actual firearms, weapon parts or explosives.

This means that the threats that Veronica and her colleagues see are in fact not found in the travellers' suitcases, but are produced by algorithms, technology developers and their depictions of *already known threats*. New and as yet un-encountered dangerous objects cannot be detected by the algorithms in Level 1, nor can they be projected on to the luggage images to train the officers to see them. The TIP algorithm therefore potentially produces another type of *visual agnosia*, since it repeatedly projects only *knowns* on to the screens and into the sight of the officers, formatting, limiting and quite possibly *deskilling* their perceptions by training them to recognize only what is already known, instead of using their own skills and intuitive sense of what could constitute possible threats.

In addition to its pre-emptive functions and its potential deskillment of the officers' senses, the TIP system, as Veronica also suggests, serves to audit the officers' performance by monitoring detected and missed instances of artificial threats. This obviously situates the TIP system within the wide range of control mechanisms that govern by numbers, to which operators in any work setting are increasingly exposed (Shore and Wright 2015; Strathern 2000). It also further strengthens the suggestion that technologies of surveillance are, if not efficient in the detection of threats to national security, then at least efficient in controlling the controllers (see also Møhl 2018).

Comparisons and conclusions

This chapter has provided four examples of systems of threat assessment that work with different types of technology and infrastructural protocols. In the control booths in Copenhagen Airport, some protocols are data- and algorithm-based, whereas others operate primarily through human sensory and cognitive proficiencies and storytelling skills. These different operations of respectively human and technological observational skills, assessing the known and perceiving the unknown, are in practice tightly interwoven. They do, however, point to significant differences in temporality: between

technological re-cognition and human cognition, and respectively between identifying known and registered threats and felons based on data and prior registration, and seeking out and imaging unknown ones based primarily on the ambiguities of encounters in the here and now. Most human sensory and mental activity is based on recognition, and the balance between perceiving knowns and discovering unknowns is finely tuned and mainly reflects different forms of human cognitive behaviour. The border guards nevertheless constantly acquire new selective tacit skills from their direct experience and from digging further into suspect or unknown objects and details to substantiate or refute their intuitions and thus broaden their individual skills and sometimes also skills they share collectively. The data provided in the control booth and the TIP system, on the other hand, pointedly demonstrate the incapacity of algorithmic foresight. Both need the intervention of human agents to pick up and connect disparate details, to foresee and imagine connections and future scenarios. In that sense, data are quite impotent when it comes to assessing the now and the future.

The ABC system of facial recognition functions within a realm of semblance and simulacres. It places the process of identification solely in the face and in the 'photographic original' with which it is compared. The floor officer giving instructions is asking the person to conform to the photo by taking off their glasses, their veil, their smile. The person – and his or her identity – is reduced to, and implied to be contained in, the face, especially in the photographic version of the original face to which the traveller must conform to pass. There is an unfathomable faith in the indexicality of the image and its direct link to a previously existing face. In identity control, however, the image becomes the original and the travellers face becomes the re-presentation in an ironic semiotic inversion of object and representation.

In all cases, trying to look like a photo or like a casually dressed young European – as Hans suggests some young migrants do, confirmed by the descriptions of migrants *en route* in Part III – amounts to conforming with and in a sense inhabiting a category (Rapport 2013). And, maybe most importantly, this points to the significance of the border guards' awareness that people can and do move between categories and that identity is not something fixed, as the logics of ID and data would imply.

The logics of the identification process also point to a hyper-focalization of the face

itself, whether original or actual, as the locus of identity. The face becomes a hyperbole, as implied in the notion of 'faciality' (Deleuze and Guattari 1987; Gates 2011) and 'the imposition on the subject to assume a 'face'' (Rodrigues 2012: 3). In that sense, the ABC is a perfect example of what Deleuze and Guattari call an 'abstract machine of faciality' – it no longer works with humans or live faces or in any way with complex human identities, but with abstract 'phantomized' template versions of both the photographed 'original' (linked to a dataset) and actual faces template-ified in the ABC.

In the ABC and the luggage scans, the technologies tend to pick out zones and objects of interest and to produce threats, for example, as TIPs and as hits, productions that format the human senses and that may produce certain forms of agnosia in the interaction between these different forms of human-technological vigilance. By 'providing more exposure to threats', as the developers say (see note 5), the TIP image ensures that officers are regularly exposed to imaginary threat so that their vision may be trained despite the lack of direct perceptions of actual weapon parts or explosives. This means that threats are not constituted by travellers and their objects, but produced by algorithms, technology developers and their assessments of *currently known* threats. The threat projections thus operate within the domain of hindsight. New and unknown, as yet unencountered dangerous objects can neither be detected by the algorithms nor projected on to the luggage images and trained by the officers.

Border control is governed by a fundamental predicament, a pervasive uncertainty that cannot be represented in numbers and audits because by definition it goes unregistered. How many persons have actually managed to pass control without the proper documentation. How many went 'under the radar'? There is no way of knowing. This prevailing *spectre of uncertainty* in border and security control sets a perfect scene for the prolific production of social imaginaries and story-telling. As we have seen, these stories are produced by assembling a variety of small cues into narratives that explain the presence and concurrence of those cues and that spell out apparent incongruities (see also Holmberg 2003). But they in no way create a full picture of who a traveller might be or have in mind – that dream of total transparency that any border guard system would like to possess and that the biometric technologies allegedly provide. Indeed, it is widely acknowledged that the technologies cannot keep that promise and that the small

details are only fragments that provide a basis only for hunches, not for truths. Indeed, the great unknown prevails and seems to fill the room around the working officers as an underlying tension in every act of decision-making they engage in. Am I making the right choice? Is the ABC making the right decision? Was that person who the passport said she was? Was that strange object in the suitcase a kitchen utensil or part of a bomb? Is the ABC working properly?

The technological infrastructure that is supposed to help the officers in their work and eliminate most of the uncertainty tends to do the exact opposite, at least from the border guard's perspective. Take, for example, the indecisiveness of the ABC. Every time it shifts from one recognition score to another, swinging back and forth between degrees of likeness and recognition, and gradually closing in on a passable recognition score, then lowering it again… – …13…35…22…44! – it very explicitly signals to the border guard looking at the screen that *it is not sure*. It also signals that likeness is a very relative and negotiable matter, a question of degree and approximation – very rarely at 100, more often oscillating between 20 and 50. So where the door to the traveller is decidedly either closed or open – either/or – the displayed, colourfully shifting recognition score is wholly ambiguous and only underscores the uncertainty of the border control endeavour. In the same manner – besides deskilling the officers' vision – every time the TIP images appear on an officer's screen, it indicates and reminds her that she and her vigilance are being controlled and are under suspicion. It places management control, suspicion and thus uncertainty at the forefront of the activity.

And basically, can we trust the ABC and its complete reliance on ID photos and likenesses? As an airline officer recently answered when I asked him what he had checked in my passport, 'I just check the date of expiration and the name.' I persisted, 'And what about the ID photo?!' 'Oh, I don't look at that. Photos can cheat.' Although facial recognition involves complex and very high-tech operations and calculations and is presented and merchandized as a new generation of biometrics – transcending both human capacities and older forms of identity verification, and thus being the ultimate high-tech solution to the quest for shatterproof border control – facial recognition can in fact be circumvented with sufficient practical skill (or economic sway). The belief in its fool-proof qualities belongs to the myth of the 'digital sublime' (Mosco 2004) and its

claims to produce definitive truths about the relationship between faces and identities (Gates, 2011) rather than radically different mechanisms of sign analysis and control.

While we should not belittle the potency of digital and data-based surveillance and border control technologies such as the ABC, we should not exaggerate it either. This chapter has, among other things, tried to examine the efficiency of a surveillance technology celebrated – or criticized, depending on the perspective – for its efficiency and capacity to create 'smarter', impenetrable borders. But, echoing Kelly Gates (2011) and William Bogard (2006), if we consider the all-powerfulness of surveillance and biometric technologies as givens, as 'already here to stay' – indeed, engaging ourselves in what Bogard calls 'the imaginary of surveillant control'–, or if we succumb to the naïve fascination of the digital sublime without also acknowledging and analysing the shortcomings and sense-making bases of such technologies, we risk contributing to the illusion of their proficiencies. The myth, with its preventive effect, becomes part of the 'fortress'. Finding a middle way by paying greater attention to the concrete processes and authoritative, semiotic premises of such technologies, especially alongside their daily users, can give us a more fine-tuned sense of their workings and of their failures to fulfil that illusion of omnipotent all-powerful surveillance and impenetrable control. What is interesting is to figure out the bases for the claims to veracity of such technologies, and the ambiguities that in practice they come to operate with and under – in this case, that it suffices to resemble a tiny photo of a face in order to pass a border.

REFERENCES

Bogard, William. 2006. "Welcome to the Society of Control: The Simulation of Surveillance Revisited." *The new politics of surveillance and visibility*: 55–78.

Coutin, Susan Bibler. 2003. "Papeles, Permisos, and Permanence." In *Legalizing Moves: Salvadoran Immigrants' Struggle for U.S. Residency*, Ann Arbor: University of Michigan Press, 49–78.

Cutler, Victoria, and Susan Paddock. 2009. "Use of Threat Image Projection (TIP) to Enhance Security Performance." *Proceedings - International Carnahan Conference on Security Technology*: 46–51.

Deleuze, Gilles, and Félix Guattari. 1987. *A Thousand Plateaus - Capitalism and Schizophrenia*. Minneapolis: University of Minnesota Press.

European Commission. 2000. Official Journal of the European Communities *Charter of Fundamental Rights of the European Union*. EU.

———. 2017. *Commission Recommendation of 12.5.2017 on Proportionate Police Checks and Police Cooperation in the Schengen Area*. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0230:FIN:EN:PDF (July 16, 2017).

European Union Agency for Fundamental Rights. 2010. *Police Stops and Minorities: Understanding and Preventing Discriminatory Ethnic Profiling*. Austria.

Feldman, Gregory. 2013. "The Specific Intellectual's Pivotal Position: Action, Compassion and Thinking

in Administrative Society, an Arendtian View." *Social Anthropology* 21(2): 135–54.
Frontex. 2013. *Frontex Evaluation Report 2013 - Joint Operation METEOR 2013 - Air Border Cooperation*. Warsaw.
Gates, Kelly. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York University Press.
Grasseni, Cristina. 2007a. "Communities of Practice and Forms of Life: Towards a Rehabilitation of Vision?" In *Ways of Knowing: Anthropological Approaches to Crafting Experience and Knowledge*, ed. Mark Harris. New York: Berghahn Books, 203–21.
———. 2007b. "Good Looking: Learning to Be a Cattle Breeder." In *Skilled Visions: Between Apprenticeship and Standards*, ed. Christina Grasseni. New York: Berghahn Books, 47–66.
———. 2018. "Skilled Vision." In *The International Encyclopedia of Anthropology*, Oxford: John Wiley & Sons, Ltd, 1–7. http://doi.wiley.com/10.1002/9781118924396.wbiea1657 (January 28, 2019).
Haraway, Donna J., Cary Wolfe, and Donna J. Haraway. 2017. "A Cyborg Manifesto." In *Manifestly Haraway*, ed. Cary Wolfe. University of Minnesota Press, 3–90.
Hofer, Franziska, and Adrian Schwaninger. 2005. "Using Threat Image Projection Data for Assessing Individual Screener Performance." *WIT Transactions on the Built Environment* 82: 417–26.
Holmberg, Lars. 2003. *Policing Stereotypes: A Qualitative Study of Police Work in Denmark*. Glienicke/Berlin: Galda + Wilch Verlag.
Jackson, Michael. 2002. "Familiar and Foreign Bodies: A Phenomenological Exploration of the Human-Technological Interface." *J. Roy. anthrop. Inst. (N.S.)* 8(2): 333–46.
Møhl, Perle. 2018. "Border Control and Blurred Responsibilities at the Airport." In *Security Blurs, the Politics of Plural Security Provision*, eds. Tessa G Diphoorn and Erella Grassiani. London: Routledge, 118–35.
———. "ID-Entities, Data and the Sensory Work of Border Control." *Ethnos*.
Mosco, Vincent. 2004. *The Digital Sublime, Myth, Power, and Cyberspace*. Cambridge, Mass.: MIT Press.
Okely, Judith. 2001. "Visualism and Landscape: Looking and Seeing in Normandy." *Ethnos* 66(1): 99–120.
Rapiscan. 2017. "Threat Image Projection." https://www.rapiscansystems.com/en/products/radiation_detection/productsrapiscan_threat_image_projection (December 4, 2017).
Rodrigues, Laurie. 2012. "Seeing Immanent Difference : Lorna Simpson and the Face ' s Affect." *Rhizomes* (23). http://www.rhizomes.net/issue23/rodrigues/rodrigues.html (August 15, 2018).
Scott, James C. 1998. "State Projects of Legibility and Simplification." In *Seeing like a State : How Certain Schemes to Improve the Human Condition Have Failed*, New Haven: Yale University Press, 9–84.
Shore, Cris, and Susan Wright. 2015. "Audit Culture Revisited." *Current Anthropology* 56(3): 421–44.
Strathern, Marilyn, ed. 2000. *Audit Cultures: Anthropological Studies in Accountability, Ethics and the Academy*. London & New York: Routledge.
Wells, Joshua J. 2014. "Keep Calm and Remain Human: How We Have Always Been Cyborgs and Theories on the Technological Present of Anthropology." *Reviews in Anthropology* 43(1): 5–34.

NOTES

[1] See, for example, Danish police authorities' guidelines for ID photos concerning postures, props and clothing: https://politi.dk/pas/krav-til-pas-og-koerekortfoto
[2] For a description of Frontex operations, see the general introduction to the present book.
[3] Profiling based especially on ethnicity is formally prohibited by European law (European Commission 2000; European Union Agency for Fundamental Rights 2010).
[4] 'TIP' images can be either virtual threat items projected into X-ray images of real passenger bags or virtual X-ray images of whole bags (Hofer and Schwaninger 2005), depending on the type of screening system. In Gibraltar both are used, depending on the security level.
[5] According to the producer of the system, 'TIP is designed to advance screener proficiency by providing more exposure to threats on a regular basis, and to track screener performance' (Rapiscan 2017).